Department of Homeland Security Daily Open Source Infrastructure Report for 27 March 2006

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

For info click here
http://www.dhs.gov/

Daily Highlights

- The U.S. Department of Agriculture's Animal and Plant Health Inspection Service is proposing to make changes to the exotic Newcastle disease domestic quarantine regulations which would help ensure that the disease does not spread and is eradicated within quarantined areas. (See item 20)
- The National Rural Water Association last week released their plan to initiate state emergency response networks to restore safe and clean drinking water and sanitation services during emergences. (See item 22)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base

Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping

Sustenance and Health: Agriculture; Food; Water; Public Health

Federal and State: Government; Emergency Services

IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard

Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *March 23, Utility Automation & Engineering* — **National Coal Council study urges more coal use.** The National Coal Council (NCC) released "Coal: America's Energy Future," a study that contains recommendations to the U.S. Secretary of Energy to maximize use of abundant coal. The study identifies ample amounts of U.S. coal reserves to support 100 gigawatts of new electricity generation, 2.6 million barrels per day of refined liquid products, and four trillion cubic feet per year of natural gas production for all applications. The study looks at supply challenges associated with imported oil and imported liquefied natural gas in addition to the explosive economic growth in China and India. To meet increased energy needs, an additional

1.3 billion tons of U.S. coal would be used annually, doubling current use. Coal is the only domestic fuel that has the flexibility and reserve base to meet future energy demand, with enough reserves to last more than a century, even at elevated levels of use, says the NCC. "The study is especially timely given recent geopolitical events and the hurricane devastation in the Gulf, which demonstrates the fragile balance between energy supply and demand," said Jeffrey D. Jarrett, U.S. Assistant Secretary of Energy. The final study will be published in April.
Source: http://uaelp.pennnet.com/Articles/Article_Display.cfm?ARTICL E_ID=250969&p=22

2. *March 23, Associated Press* — **U.S. hires Hong Kong firm to run nuclear detectors at Bahamas port.** The U.S. government is hiring a Hong Kong conglomerate to help detect nuclear materials inside cargo passing through the Bahamas to the U.S. and elsewhere. The no−bid contract with Hutchison Whampoa Ltd. represents the first time a foreign company will be involved in running a sophisticated U.S. radiation detector at an overseas port without American customs agents present. The contract is currently being finalized.
Source: http://cnews.canoe.ca/CNEWS/World/WarOnTerrorism/2006/03/23/ 1502493−ap.html

3. *March 23, Reuters* — **U.S. OKs tolls for Canada crude pipeline expansion.** U.S. regulators have approved the proposed tolls for the Southern Access oil pipeline expansion project that will increase the amount of Canadian crude oil that can be shipped south by 400,000 barrels per day. The expansion would add a substantial amount of new export capacity for Canadian oil producers. Canada exported about 1.6 million barrels per day to the U.S. in 2004, most of which came by pipeline from Alberta. The Southern Access project is an expansion of the existing crude oil pipeline networks of Canada's Enbridge and its U.S. affiliate Enbridge Energy Partners LP between Hardisty, Alberta and Flanagan, Illinois. The Federal Energy Regulatory Commission decision allows Enbridge and EEP to apply a surcharge to the existing rates on the Lakehead oil pipeline system in the U.S. to cover the costs associated with the $1 billion project.
Source: http://news.yahoo.com/s/nm/20060323/wl_canada_nm/canada_ener gy_pipeline_enbridge_col_1

4. *March 23, Associated Press* — **Two hurt in blaze at Japanese nuclear power plant.** Investigators on Thursday, March 23 were looking into what caused a four−hour blaze at a nuclear power plant in western Japan that left two employees slightly injured. No radiation leaked from the Oi power plant in Fukui prefecture during the Wednesday, March 22 fire, but two workers were hospitalized with smoke inhalation injuries. The cause of the fire was under investigation, but it seemed to have started in the waste incineration part of the plant, Manabu Kobana of Kansai Electric Power Co. Smoke was seen pouring out of the facility and firefighters were unable to get close to the flames for two hours because of the dense smoke. It took them another two hours to put out the fire, according to local officials. All four pressurized water reactors at Oi, some 240 miles west of Tokyo, were operating normally and there was no radiation leakage, Kansai Electric Power said. Sensors inside and around the plant also showed no signs of radiation, police confirmed.
Source: http://www.aberdeennews.com/mld/miamiherald/news/world/14163 990.htm?source=rss&channel=miamiherald_world

5. *March 22, Reuters* — **Kansas to let nuclear plant guards shoot to kill.** Kansas Governor Kathleen Sebelius signed a bill on Wednesday, March 22 authorizing security guards to shoot

to kill to protect the state's lone nuclear power plant. "There's no doubt that nuclear facilities are a potential target for terrorists...Kansas has one nuclear plant, Wolf Creek, and we must make sure it's properly protected. Allowing guards to use deadly force in certain circumstances increases the security of the plant, and of our state," said Sebelius. Texas and Arizona have similar laws.
Source: http://go.reuters.com/newsArticle.jhtml?type=domesticNews&storyID=11629818&src=rss/domesticNews

[Return to top]

Chemical Industry and Hazardous Materials Sector

6. *March 24, Sun−Sentinel (FL)* — **Gas tanker overturns, shuts down interstate.** A fatal accident shut down both the north and southbound lanes of Interstate−95 early Friday morning, March 24, after a loaded gas tanker overturned, the Florida Highway Patrol said. The tanker was carrying more than 8,000 gallons of fuel.
Source: http://www.sun−sentinel.com/news/local/florida/sfl−324i95crash,0,7434505.story?coll=sfla−news−florida

[Return to top]

Defense Industrial Base Sector

7. *March 24, U.S. Department of Defense* — **Report provides strategic vision for countering WMD.** A document released Friday, March 24, outlines the Department of Defense's (DoD) strategy for combating weapons of mass destruction (WMD) and will serve as the foundation for assigning specific responsibilities throughout DoD toward that goal, a senior military official said. The "National Military Strategy for Combating Weapons of Mass Destruction" deals with "the greatest risk" confronting the United States and other free societies, Army Brig. Gen. Robert Caslen Jr., the Joint Staff's deputy director for the war on terror, said. "And that's weapons of mass destruction in the hands of terrorists," he said. The document outlines DoD's role in the U.S. government effort to counter the WMD threat and the role the department would play in fulfilling the president's National Strategy to Combat Weapons of Mass Destruction, released in 2002.
National Military Strategy to Combat Weapons of Mass Destruction:
http://www.defenselink.mil/pdf/NMS−CWMD2006.pdf
Source: http://www.defenselink.mil/news/Mar2006/20060324_4592.html

8. *March 23, U.S. Army* — **Army, Air Force announce joint cargo aircraft program.** Army and Air Force officials announced Friday, March 17, that a new Joint Cargo Aircraft, designed to enhance the combat readiness of both services, will be developed by a combined team. Fielding of the new aircraft is expected within two years. The Request for Proposals was released March 17 after the Acquisition Strategy Report was signed that morning, according to Pentagon officials. A Joint Program Office, comprised of personnel from both branches of service, will open October 1 in Huntsville, AL, with the Army taking the lead.
Source: http://www4.army.mil/ocpa/read.php?story_id_key=8731

[Return to top]

Banking and Finance Sector

9. *March 24, Finextra* — **Data security top risk concern in outsourcing.** Data security has become the top risk concern for U.S. companies considering outsourcing operations to service providers, according to a study by management consultant Booz Allen Hamilton. The survey of 158 U.S. senior executives from a variey of industries found that the vast majority of respondents −− 91 percent −− were 'somewhat' or 'very concerned' about data theft or misuse in outsourced operations. Information security is one of the top three most important factors in selecting an outsourcing partner, chosen by 50 percent of respondents, ahead of financial strength, business stability, and reputation. Nearly 70 percent of respondents also said they were reviewing their outsourcing strategy in response to hearing of recent high profile cyber crime, customer data theft, and network security incidents. Around three quarters of respondents perceive a higher security risk with offshore firms, rather than domestic providers. While data theft is a top issue when outsouring, terrorism is viewed as a 'moderate' to 'serious' threat by 48 percent of respondents. Only 35 percent feel that physical breaches and natural disasters are a major concern.
   Source: http://finextra.com/fullstory.asp?id=15097

10. *March 24, Websense Security Labs* — **Phishing Alert: President's Choice Financial.** Websense Security Labs has received reports of a new phishing attack that targets customers of President's Choice Financial. Users receive a spoofed e−mail message, which claims that their account information needs to be verified due to new security measures. The message provides a link to a phishing Website. Users who visit this Website are prompted to enter personal and account information.
   Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =450

11. *March 23, NBC 4 (DC)* — **Identity theft possible at D.C. elections office.** The D.C. elections office may have compromised thousands of residents' personal information to identity theft. The elections office contains more than 300,000 registered names on voter rolls. The indexes include details like addresses, birthdates, Social Security numbers, and voter information. Until recently, the information printed out included social security numbers that could easily be read, increasing the chance of identity theft. Printing the numbers out clearly is a violation of federal law. "We are whiting out the Social Security number on any data that's given out to the public," Bob Ofield of the D.C. elections office said. The elections spokesperson said although the office had routinely blotted out Social Security numbers, they could still be read with a little effort. Reporter Mark Segraves obtained the numbers of high−ranking officials like Mayor Anthony Williams.
   Source: http://www.nbc4.com/news/8217746/detail.html?rss=dc&psp=news

12. *March 22, Federal Times* — **Thrift Savings Plan system appears unharmed by e−mail scam.** The Thrift Savings Plan (TSP) program is operating normally after plan operators halted transactions temporarily in response to an e−mail scam that targeted some of the 3.6 million TSP participants. The e−mail purportedly sent from the address accounts@tsp.gov informed users that an e−mail address had been added to their accounts and instructed them to contact

TSP customer service with any questions by clicking on a link provided. The link took users to a bogus version of the TSP account access screen, where they were asked to enter their Social Security numbers and the four−digit personal identification number used to access their accounts. Users were then taken to another Web page where they were asked for credit card and bank account numbers. Hours after learning of the bogus e−mail Thursday, March 16, TSP officials shut down the portion of the Website that allows applicants to transfer funds among accounts, withdraw funds, or apply for loans. Operations resumed within 24 hours. “We don’t have any reason to believe any TSP account was breached,” said Gary Amelio of the Federal Retirement Thrift Investment Board, which manages TSP. The FBI is continuing to investigate.
Source: http://federaltimes.com/index.php?S=1634027

[Return to top]

Transportation and Border Security Sector

13. *March 24, Associated Press* — **Venezuela, U.S. said to avoid proposed airline ban.** The U.S. and Venezuela have reached a temporary agreement that will avoid a proposed ban on flights by most U.S. airlines to the South American country, the U.S. ambassador said. William Brownfield said Thursday, March 23, that officials from both countries agreed to have the U.S. Federal Aviation Administration work with Venezuelan officials to improve local safety standards. Venezuelan authorities want the FAA to end safety restrictions that prevent Venezuelan airlines from flying to the United States and had warned that they would decide on March 30 whether to ban U.S. flights. The proposed ban would have prohibited all flights by Houston−based Continental Airlines and Atlanta−based Delta Air Lines. It would have restricted some by Fort Worth−based AMR's American Airlines, the largest U.S. carrier. Brownfield had warned last week that Venezuelan flights to the United States would be banned if Venezuela prohibited flights by U.S. airlines.
Source: http://www.usatoday.com/travel/flights/2006−03−24−venezuela− ban_x.htm

14. *March 23, Star Bulletin (HI)* — **New airline go! begins flights this summer.** Mesa Air Group Inc.'s much−anticipated expansion into Hawaii as an interisland carrier will be a "go!" as of June 9, with one−way fares starting at $39. The company unveiled its to−the−point name and logo go! Wednesday, March 22 and began taking reservations. The carrier is expected to change Hawaii's interisland air travel market by providing cost−weary consumers with more choice, and has already prompted an industry fare war. Jonathan Ornstein, chairman and chief executive officer of Mesa Air Group, said he expects to shore up island business by tapping a niche market of Hawaii residents and business people who had cut back on flying between the islands because of prohibitive ticket prices. Wednesday night, Aloha and Hawaiian airlines announced they were lowering fares to $39.
Source: http://starbulletin.com/2006/03/24/news/story02.html

15. *March 23, National Journal* — **Informal survey shows lax ID checks for air travelers.** An informal survey of more than 80 domestic airline travelers found that Transportation Security Administration (TSA) officials often do not enforce the agency's own rule that travelers must present government−issued identification at airports. The TSA rule mandates that airline travelers present at least one form of such ID at security checkpoints. Many of those who recounted their experiences at the airports when they had forgotten their identification or it was

stolen, or their driver's licenses had expired, said TSA screeners subjected them to extra security checks but allowed them to board the aircraft. Other travelers were allowed to board planes after showing several forms of non−government identification, such as credit cards or school ID cards. The survey was undertaken by a group called "The Identity Project." The survey was completed by people who responded to the group's request for information about their experiences at airports when they had traveled without any forms of identification deemed valid by TSA.
Source: http://www.govexec.com/story_page.cfm?articleid=33681&dcn=to daysnews

16. *March 22, Associated Press* — **Hooters chairman uncertain about airline's future.** The owner of Hooters Air is uncertain about the airline's future but he stopped short of saying it would soon shut down. Robert Brooks said he is "open for suggestions" over what to do about the ailing airline. Hooters Air has trimmed service to some airports and ran up fuel service bills. Airline industry analyst Tim Sieber said problems for the airline range from a highly competitive low−fare airline industry to rising fuel prices.
Source: http://www.usatoday.com/travel/flights/2006−03−22−hooters−fu ture_x.htm

17. *March 22, USA TODAY* — **World airline industry recovering.** Rising fares and falling labor costs in the USA, plus improving economic conditions elsewhere, are speeding the recovery of the global airline industry. Giovanni Bisignani, director general of the International Air Transport Association, said Wednesday, March 22 that he now expects airlines globally to lose only $2.2 billion this year, a better performance than his previous projection of a $4.3 billion loss. In 2007, the industry should earn $7.2 billion, up from a prior projection of a $6.2 billion profit. "While the trend is positive, we are nowhere near sustainability," Bisignani said. Airlines globally have lost more than $50 billion since 2000, including about $40 billion by U.S. carriers. Bisignani said improved economic prospects in Europe and Asia, along with improving conditions in the U.S.'s air travel market, give him reason for some optimism.
Source: http://www.usatoday.com/money/biztravel/2006−03−22−airline−i ndustry−profit_x.htm

[Return to top]

Postal and Shipping Sector

18. *March 24, News Press (FL)* — **Suspicious powder prompts mail center evacuation in Florida.** More than 200 postal workers in south Fort Myers, FL, were evacuated from a distribution center Thursday, March 23, after a sorting clerk spotted powdery residue on a letter. It was later determined the white powder was insecticide sent by a mother to her son in Cape Coral, postal officials said. The incident shut down the plant for nearly two hours. Prior to this incident, the letter had gone through a biohazard detection system and a mail plant in Tampa without raising alarm.
Source: http://www.news−press.com/apps/pbcs.dll/article?AID=/2006032 4/NEWS0117/603240392/1075

[Return to top]

Agriculture Sector

19. *March 25, Richmond Times Dispatch (VA)* — **Peanuts shrinking in Virginia.** More and more, farmers in the southeastern Virginia localities where peanuts are grown −− Dinwiddie, Greenville, Isle of Wight, Prince George, Southampton, Surry, Sussex and Suffolk −− are deciding not to grow peanuts. Five years ago, growers planted 75,000 acres of peanuts. Last year, that dropped to 23,000 acres. One Virginia Tech economist estimates that this year's crop will take only 15,000 acres. Peanut production in Virginia dropped sharply after Congress passed the 2002 farm bill, which did away with a long−standing quota and price−support program and replaced it with an Agriculture Department program more akin to those for wheat and corn growers. In the final year of the quota program, the federal support price for Virginia peanuts was roughly $610 per ton, but last year under the new program it was $355 per ton, a figure tied to world market prices. As recently as 1995, Virginia peanut growers were guaranteed $678 per ton for their harvested quota of peanuts. The Virginia−type of gourmet snack peanut −− one of four varieties in the U.S. −− has been grown primarily in Virginia and eastern North Carolina.
    Source: http://www.timesdispatch.com/servlet/Satellite?pagename=RTD%2FMGArticle%2FRTD_BasicArticle&c=MGArticle&cid=1137834932731&path=!business&s=1045855934855

20. *March 24, Animal and Plant Health Inspection Service* — **Change to domestic quarantine regulations regarding exotic Newcastle disease proposed.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) is proposing to make several changes to the exotic Newcastle disease (END) domestic quarantine regulations. The proposed changes include harmonizing the foreign and domestic regulations regarding the movement of dressed carcasses of dead birds and dead poultry; adding restrictions on the interstate movement of ratites out of quarantined areas; providing for the use of alternative procedures for treating manure and litter for composting, and adding an additional surveillance period prior to removing quarantine restrictions. APHIS has determined that these changes are necessary based on experiences during the eradication programs for the recent outbreaks of END in California, Arizona, Nevada and Texas. These changes would help ensure that END does not spread and is eradicated within quarantined areas. Exotic Newcastle disease is a highly contagious and fatal viral disease that affects all species of birds. It affects the respiratory, nervous and digestive systems of birds, and many birds die before demonstrating any clinical signs of the disease.
    Source: http://www.aphis.usda.gov/newsroom/content/2006/03/endregs.s html

[Return to top]

Food Sector

21. *March 24, Agricultural Research Service* — **Canada adopts method to extract noroviruses from oysters.** Several agencies responsible for public health oversight in Canada recently adopted a technique based on research by Agricultural Research Service (ARS) scientists to extract and test noroviruses in oysters. Noroviruses, which cause approximately 23 million illnesses each year, are the leading cause of nonbacterial acute gastroenteritis outbreaks. The

method effectively separates and purifies norovirus genetic materials from within oyster tissues. Oysters, clams and mussels have caused numerous outbreaks of norovirus illness. Symptoms of the illness include potentially severe diarrhea, vomiting or both that develop usually within a day after consuming contaminated food or drink. In 2002, the ARS researchers published an article on the successful use of the method to detect both hepatitis A virus and norovirus in Asian clams implicated in an outbreak of norovirus illness in New York State.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

[Return to top]

Water Sector

22. *March 23, National Rural Water Association* — **Disaster guide will help small water systems.** The National Rural Water Association (NRWA), the country's largest community−based water organization released their plan to initiate state emergency response networks to assist community water and sanitation supplies during emergencies. The "Rural Water Mutual Aid Agreement" and "A State Wide Water and Wastewater Utility Emergency Support Network" guide describes actions, measure, approaches, and tactics that were developed based on the NRWA's Emergency Response Committee recommendations and the lessons learned from hurricane emergency responses in Florida, Texas, Mississippi, Alabama, and Louisiana. The plan details how communities can implement the most successful emergency response network to restore safe and clean drinking water and sanitation services during emergences.
NRWA Guide: http://www.ruralwater.org/emergencynetwork.pdf
Source: http://www.ruralwater.org/emergencynetworkrelease.pdf

[Return to top]

Public Health Sector

23. *March 26, Associated Press* — **China confirms woman's bird flu death.** A woman who died in Shanghai tested positive for the H5N1 strain of bird flu, China announced Saturday, March 25. The woman who died in Shanghai was the Chinese mainland's 11th human death from bird flu and the first in Shanghai, the country's biggest city, according to the World Health Organization. The migrant worker, identified only by the common surname Li, died Tuesday, March 21, after being hospitalized with fever and cold symptoms.
Source: http://abcnews.go.com/Health/wireStory?id=1769253

24. *March 26, Agence France−Presse* — **Indonesia confirms girl died of bird flu.** The girl, a resident of West Jakarta, died Thursday, March 23, at Jakarta's Sulianti Saroso hospital, the main center for bird flu patients, health ministry official Hariyadi Wibisono said. Samples from the girl have been sent to a Hong Kong laboratory accredited by the World Health Organization for confirmation. If confirmed, the girl would be Indonesia's 23rd bird flu fatality. Results from local tests are usually accurate.
Source: http://www.forbes.com/work/feeds/afx/2006/03/26/afx2622030.h tml

25. *March 24, Reuters* — **Children in Somalia stricken with polio.** Nearly 200 children in Somalia have been paralyzed with polio since the disease re−emerged in July, and the virus is spreading in the lawless country, the World Health Organization (WHO) said on Friday, March 24. A nationwide vaccination campaign is being launched on Sunday, March 26, to try to reach 1.4 million Somali children under age five. Four in five of the cases since July were recorded in the capital Mogadishu, where the virus now seems to be on the decline after immunization campaigns, but it has spread to Lower Juba in the south and Mudug in the northeast, the WHO said. In all, the crippling virus is now been reported in eight of Somalia's 19 regions.
Source: http://today.reuters.com/news/newsArticle.aspx?type=healthNews&storyID=2006−03−24T134602Z_01_L24771100_RTRUKOC_0_US−SOMALIA−POLIO.xml&archived=False

26. *March 23, Reuters* — **Drug−resistant tuberculosis rising.** Federal health officials on Thursday, March 23, said drug−resistant strains of tuberculosis infection were rising, posing major challenges to efforts to eliminate the disease. The U.S. Centers for Disease Control and Prevention (CDC) reported that cases of tuberculosis that were resistant to the two drugs considered the first−line of treatment rose 13 percent to 128 in the U.S. between 2003 and 2004, the highest yearly increase since 1993. Of those 128 people, 97 were born outside the U.S., in countries such as Mexico and Vietnam.
CDC Fact Sheet: http://www.cdc.gov/od/oc/media/pressrel/fs060323.htm
Source: http://www.alertnet.org/thenews/newsdesk/N23262071.htm

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

27. *March 25, The Graphic (CA)* — **Malibu plans for disaster.** The city of Malibu, CA, is preparing residents for the case of a tsunami by creating a preparedness plan, informing citizens of the chances and consequences of such a disaster. Brad Davis, coordinator of emergency preparedness at Malibu City Hall, said that if a tsunami threatened Malibu, all coastline structures, especially in the eastern−most half of the city would be in jeopardy. There is no siren for early warning. “The city of Malibu would be notified by the Alaska/Hawaii warning network within minutes of an event that could remotely have an effect on this area, but getting the warning out to the population would take time,” according to the Emergency Response Plan manual. The manual indicates that any area that is 90 feet above sea level may be considered an area safe from tsunami upsurge. Pepperdine is about 100 feet above sea level.
Source: http://graphic.pepperdine.edu/news/2006/2006−03−23−diasterpl an.htm

28. *March 24, Berkeley Daily Planet (CA)* — **Officials discuss disaster preparedness.** Top state, county and city emergency services officials from the State of California and Alameda County met with senior officials from the University of California−Berkeley, Lawrence Berkeley

National Lab, Alta Bates Summit Medical Center, Vista College, the Berkeley Unified School District and Bayer Health care Thursday, March 23, to discuss emergency preparedness coordination and communication plans in the event of a major disaster in Berkeley. Speaking to members of the media after the briefing session, Berkeley Mayor Tom Bates said that in the event of a major disaster, the City of Berkeley's Public Safety Building would be converted into a command center. He added that federal and state agencies would be carrying out emergency services throughout Berkeley and jointly making decisions on healthcare and evacuation services. In the event that cell phone services were disrupted, bicycle dispatchers would be sent out to act as messengers between city officials. There is also talk of using ham radios.
Source: http://www.berkeleydaily.org/text/article.cfm?issue=03−24−06 &storyID=23721

29. *March 23, Federal Computer Week* — **New Orleans wants regional, redundant radio system.** New Orleans officials are hoping to have their radio communications network linked regionally and to a statewide system by June 1, the start of the 2006 hurricane season. City government officials and first responders have been working toward connecting their 800 MHz radio system within Orleans Parish and the surrounding parishes −− Jefferson, St. Bernard and Plaquemines −− and with the state police system to provide redundancy.
Source: http://fcw.com/article92717−03−23−06−Web

30. *March 23, National Journal* — **Department of Homeland Security projects aimed at communications upgrade.** The Department of Homeland Security is preparing to deploy initiatives in the next several months aimed at ensuring state and local public−safety agencies have communications equipment that works across jurisdictions. David Boyd, director of the Office for Interoperability and Compatibility, said during a press briefing on Thursday, March 23, that the department's SAFECOM program plans to release an updated list of technology for communications equipment in April and then conduct the first national survey to gauge the interoperability of the equipment. The survey also will gauge how local and state governments are using the SAFECOM statement of requirements version 1.0, which lists technology that should be procured in order to build compatible systems.
SAFECOM program Website: http://www.safecomprogram.gov/SAFECOM/
Source: http://www.govexec.com/story_page.cfm?articleid=33683&dcn=to daysnews

[Return to top]

Information Technology and Telecommunications Sector

31. *March 24, Security Focus* — **Apache Mod_SSL SSLVerifyClient restriction bypass vulnerability.** Apache 2.x mod_ssl is prone to a restriction bypass vulnerability. This issue presents itself when mod_ssl is configured to be used with the 'SSLVerifyClient' directive.
Analysis: This issue allows attackers to bypass security policies to gain access to locations that are configured to be forbidden for clients without a valid client certificate. A complete list of vulnerable products is available within the source advisory:
http://www.securityfocus.com/bid/14721/info
For complete solution details: http://www.securityfocus.com/bid/14721/solution
Source: http://www.securityfocus.com/bid/14721/references

32. *March 24, Security Focus* — **Linux kernel SDLA IOCTL unauthorized local firmware access vulnerability.** The Linux kernel is susceptible to a local access validation vulnerability in the SDLA driver. Analysis: This issue allows local users with the 'CAP_NET_ADMIN' capability, but without the 'CAP_SYS_RAWIO' capability, to read and write to the SDLA device firmware. This may cause a denial−of−service issue if attackers write an invalid firmware. Other attacks may also be possibly by writing modified firmware files. For a complete list of vulnerable products: http://www.securityfocus.com/bid/16304/info
For solution details: http://www.securityfocus.com/bid/16304/solution
Source: http://www.securityfocus.com/bid/16304/references

33. *March 24, Security Focus* — **Linux kernel IP6_Input_Finish remote denial−of−service vulnerability.** Linux kernel is prone to a remote denial−of−service vulnerability. Analysis: A flaw in network IGMP processing that a allowed a remote user on the local network to cause a denial−of−service disabling of multicast reports if the system is running multicast applications. For a complete list of vulnerable products: http://www.securityfocus.com/bid/16043/info
Solution: Vendor updates are available. For solution details:
http://www.securityfocus.com/bid/16043/solution
Source: http://www.securityfocus.com/bid/16043/references

34. *March 24, eWeek* — **Do−it−yourself spyware kit sells for $20.** A do−it−yourself malware creation kit is being hawked on a Russian Website for less than $20, according to security researchers tracking the seedier side of the Internet. Virus hunters at SophosLabs discovered the spyware kit, called WebAttacker, on a Website run by self−professed spyware and adware developers. The WebAttacker kit includes scripts that simplify the task of infecting computers and spam−sending techniques to lure victims to specially rigged Websites.
Source: http://www.eweek.com/article2/0,1895,1942497,00.asp

35. *March 23, Secunia* — **KisMAC Cisco vendor tag SSID parsing buffer overflow.** A vulnerability exists in KisMAC, which potentially can be exploited by malicious people to compromise a user's system. Analysis: The vulnerability is caused due to a boundary error in the "WavePacket:parseTaggedData()" function when parsing the Cisco vendor tag for additional SSIDs in a received 802.11 management frame. This can be exploited to cause a stack based buffer overflow and potentially allows arbitrary code execution. Successful exploitation requires that the user is e.g. tricked into opening a malicious pcap file containing special crafted management frames, or via raw management frames that are sent onto the wireless network while the user is performing a passive network scan. Vulnerable software: KisMAC 0.x.
Solution: Update to version R73p: http://kismac.de/download.php
The vulnerability has also been fixed in developer version 113.
Source: http://secunia.com/advisories/19354/

36. *March 23, Security Tracker* — **VeriSign Managed PKI input validation flaw in 'haydn.exe' permits cross−site scripting attacks.** A vulnerability was reported in VeriSign's Managed PKI. A remote user can conduct cross−site scripting attacks. Analysis: The 'haydn.exe' script does not properly filter HTML code from user−supplied input before displaying the input. A remote user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. The code will originate

from the site running the Managed PKI software and will run in the security context of that site. As a result, the code will be able to access the target user's cookies (including authentication cookies), if any, associated with the site, access data recently submitted by the target user via Web form to the site, or take actions on the site acting as the target user. Affected version: 6.0. Solution: The vendor indicates that, as a solution, a default HTML file must be constructed by creating a blank html file in the '/htmldocs/' directory labeled 'fdf_noHTMLFile.html'.
Source: http://securitytracker.com/alerts/2006/Mar/1015813.html

37. *March 23, Internet Security Systems* — **IBM Tivoli Business Systems Manager apwc_win_main.jsp skin parameter cross−site scripting.** IBM Tivoli Business Systems Manager version 3.1 is vulnerable to cross−site scripting. Analysis: This issue is caused by improper validation of user−supplied input by the apwc_win_main.jsp script. A remote attacker could exploit this vulnerability using the "skin" parameter to execute script in a victim's Web browser within the security context of the hosting Website, allowing the attacker to steal the victim's cookie based authentication credentials. Platforms affected: Hewlett−Packard Company: HP−UX Any version; IBM: AIX Any version; IBM: IBM Tivoli Business Systems Manager 3.1; IBM: z/OS Any version; Microsoft Corporation: Windows 2000 Any version; Microsoft Corporation: Windows NT 4.0; Sun Microsystems: Solaris Any version.
Solution: Refer to IBM Technical Support Document OA14904 for patch, upgrade, or suggested workaround information:
http://www−1.ibm.com/support/docview.wss?uid=swg1OA14904
Source: http://xforce.iss.net/xforce/xfdb/25412

38. *March 23, Tech Web* — **Microsoft warns of dangerous Internet Explorer exploit.** An exploit for a new zero−day bug in Internet Explorer appeared Thursday, March 23, causing security companies to ring alarms and Microsoft to issue a security advisory that promised it would patch the problem. Just a day after anti−virus vendors warned of a new zero−day vulnerability in Internet Explorer −− the second such alert since Friday, March 17 −− companies including Symantec and Secunia boosted security levels as news of a public exploit spread. Although the publicly−posted exploit only launches a copy of the Windows calculator, "replacing the shellcode in this exploit would be trivial even for an unskilled attacker," Symantec continued. Microsoft confirmed the severity of the bug and the success of the exploit in its own advisory, issued late Thursday.
Microsoft advisory: http://www.microsoft.com/technet/security/advisory/917077.ms px
Source: http://www.techweb.com/wire/security/183702421

39. *March 23, Government Accountability Office* — **GAO−06−328: Information Security: Continued Progress Needed to Strengthen Controls at the Internal Revenue Service (Report).** The Internal Revenue Service (IRS) has a demanding responsibility in collecting taxes, processing tax returns, and enforcing the nation’s tax laws. It relies extensively on computerized systems to support its financial and mission−related operations. Effective information security controls are essential for ensuring that information is adequately protected from inadvertent or deliberate misuse, disruption, or destruction. As part of its audit of IRS’s fiscal year 2005 financial statements, the Government Accountability Office (GAO) assessed (1) the status of IRS’s actions to correct or mitigate previously reported information security weaknesses at two sites and (2) whether controls over key financial and tax processing systems located at the facilities are effective in ensuring the confidentiality, integrity, and availability of

financial and sensitive taxpayer data. GAO recommends that the IRS Commissioner take several actions to fully implement an information security program. In commenting on a draft of this report, IRS concurred with our recommendations.
Highlights: http://www.gao.gov/highlights/d06328high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−328

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis:
US−CERT is aware of a vulnerability in the way Microsoft Internet Explorer handles the createTextRange() DHTML method. By persuading a user to access a specially crafted webpage, a remote, unauthenticated attacker may be able to execute arbitrary code on that user's system. This vulnerability can also be used to crash Internet Explorer. We are aware of proof of concept code for this vulnerability. More information about the reported vulnerability can be found in US−CERT VU#876678 Microsoft Internet Explorer createTextRange() vulnerability:
http://www.kb.cert.org/vuls/id/876678

Known attack vectors for this vulnerability require Active Scripting to be enabled in Internet Explorer. Disabling Active Scripting will reduce the chances of exploitation. Until an update, patch or more information becomes available, US−CERT recommends disabling Active Scripting as specified in the Securing Your Web Browser document:
http://www.us−cert.gov/reading_room/securing_browser/#how_to_secure

TSP Phishing Scams: US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. Specifically, sites that provide online benefits are being targeted. Recently, the phishing scam targeted the Thrift Savings Plan (TSP), a retirement savings plan for United States government employees and members of the uniformed services. For more information please see Thrift Savings Plan (TSP) at:
http://www.tsp.gov/

If you were affected by the TSP phishing scam, please refer to the TSP E−mail scam instructions for assistance:
http://www.tsp.gov/curinfo/emailscam.html

US−CERT encourages users to report phishing incidents based on the following guidelines:

* Federal Agencies should report phishing incidents to US−CERT.

http://www.us−cert.gov/nav/report_phishing.html

* Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online: http://onguardonline.gov/phishing.html

Additionally, users are encouraged to take the following measures to prevent phishing attacks from occurring:

* Do not follow unsolicited web links received in email messages.

* Contact your financial institution immediately if you believe your account and/or financial information has been compromised.

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 25 (smtp), 445 (microsoft−ds), 41170 (−−−), 65520 (−−−), 32459 (−−−), 4672 (eMule), 55620 (−−−), 135 (epmap) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

40. *March 25, Southern Pines Pilot (NC)* — **Drill tests new security at school.** Almost 100 students and teachers from all three Moore County, NC, high schools participated in an emergency training drill at Union Pines to allow law−enforcement and emergency personnel to test a new, wireless security camera system that has been installed at the school. Students pretended to be wounded, trapped or held hostage. During the drill, Sgt. Bryan Monroe with the Sheriff's Office Response Team, watched the cameras on a laptop in the command center, as groups of officers in black uniforms entered the schools under the scenario that an armed intruder was on campus and had taken hostages. The Moore County school system is partnering with the Carthage Police Department and Moore County Sheriff's Office to share the wireless technology that allows law−enforcement officers, firefighters and other emergency personnel to view school security cameras as they respond to school emergencies. The Safe Schools initiative is the first collaboration between the school system and the local law−enforcement and emergency agencies for security on campus.
Source: http://www.thepilot.com/news/032606Security.html

[Return to top]

General Sector

Nothing to report.

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer